The Devil and the Details

Quantum cryptography has yet to deliver a truly unbreakable way of sending messages. Quantum entanglement may change that

Sep 21st 2013 The Economist

RECENT revelations of online snooping on an epic scale, by government agencies which may well have been breaking the law, have prompted some users of the internet to ask who you can trust with sensitive data these days. According to Artur Ekert, an Oxford academic who moonlights as director of the Centre for Quantum Technologies (CQT) in Singapore, one possibility is a defunct Irish physicist called John Stewart Bell.

In 1964 Bell proposed a test to settle once and for all whether quantum mechanics really is as weird as it famously appears to be, in that it allows for instantaneous communication between two particles, no matter how far apart they are, on condition that they were once entangled together in the same place. The short answer, as experiments carried out over subsequent decades have shown, is yes, it is. Bell's test, however, also led physicists like Dr Ekert to a remarkable insight: made sufficiently sensitive the Bell test could be used to guarantee perfectly secure communication—even if the equipment used to send and receive those communications had been sold to you by a manufacturer subverted by your enemies.

The current way quantum theory is employed in cryptography, known as "prepare and measure", works by distributing a secret key, encoded in the way light is polarised, to two people (known conventionally as Alice and Bob) who wish to talk privily with each other. This key is used to encrypt a message so that it cannot be understood, even if it is intercepted. Prepare-and-measure looks good in theory because an eavesdropper (Eve) listening in will perforce give herself away by measuring the light's polarisation, and thus disrupting the system. If that happens, Alice and Bob can ditch the compromised key and ask for another.

However, if Eve can somehow tinker with the sending and receiving equipment (for example by blinding it with a special kind of laser, as happened in one famous quantum hack in 2010, or getting the manufacturer to do something similar), she can hide her disruption, leaving Bob and Alice none the wiser. The technique therefore ceases to be secure. Given recent revelations about Western-government activities in this area, and strong suspicions about pressure the Chinese government puts on the country's computer and telecoms firms, users' fears that their equipment might not be all it says it is are hardly paranoid. The Bell test promises to assuage those fears. For whom the Bell tallies

Bell-based cryptography also works by generating a key based on the polarisation of light. But it begins by using a special machine to produce the particles of light (called photons) in which the message will be encoded. This machine turns them out as entangled pairs. One member of each pair goes to Alice, and one to Bob. For each photon she receives, Alice chooses at random which of two predetermined polarisation angles to measure. For each measurement, she can get one of two results: either the photon will appear aligned with her polarisation axis (call that a one) or

perpendicular to it (call it zero). This can be used to encode a digital bit. Bob, for his part, also measures his photon's polarisation. Both of his axes, too, have been arbitrarily set.
Conventional odds in the world of classical physics predict Alice's and Bob's bits will match three times out of four. Add in quantum entanglement, though, and the odds increase to just over 85%. This was the essence of Bell's insight.

If Alice and Bob's measurements agree more often three-quarters of the time, it suggests their photons are entangled. That means they cannot have been intercepted, since any attempt by Eve to do so would inevitably cause them to untangle. If Alice and Bob then each add a third, identical polarisation angle, they can use this extra bit, which they know they must share, to encode the cryptographic key.

The trick is to turn this insight into a practical device, given that 85% is a theoretical maximum that real-world equipment never achieves, because it does not always succeed in turning out entangled photon pairs and may also mislay some of those it does. Christian Kurtsiefer and Valerio Scarani, two of Dr Ekert's colleagues at CQT, have been trying to deal with this. Their photodetectors reach efficiencies of 97-98% and their sources of entangled photons are now "pretty much perfect", Dr Ekert says—producing unentangled pairs less than 1% of the time. The main remaining problem is losses in the fibres, filters, lenses and polarisers that link the source of entangled photons to the detectors. The more such optics there are, the lower the efficiency tends to be. For a system that goes beyond a laboratory bench efficiency quickly drops to 70-80%, which is below the 82% that theory suggests is the minimum needed if the Bell test is to be valid.

A team led by Paul Kwiat of the University of Illinois at Urbana-Champaign is trying to deal with this not by reducing the losses but rather by reducing the sensitivity of the system to such losses. Dr Kwiat attempts this by entangling photons in a slightly different, weaker way. Thus entangled, they are more vulnerable to measurement errors but more stable against losses. Last month the team presented their findings to the third International Conference on Quantum Cryptography, in Waterloo, Ontario. They think they have managed to design and implement a scheme in which 75% efficiency is enough to ensure the validity of the Bell test.
Allison Rubenok and her colleagues at the University of Calgary, in Alberta, and Liu Yang and Chen Tengyun, from the University of Science and Technology of China, use yet another approach. Each group introduces a third party who sits between Alice and Bob.

In this scheme, rather than creating and sending entangled photons, Alice and Bob begin by polarising their light pulses at random. Each then sends his or her pulse, whose polarisation is known only to the sender, to the third party, who performs a variant of the Bell test on the two incoming signals. The outcome is successful for those combinations of photons from Alice and Bob that are in the same quantum state. These outcomes do not need to be secret: once publicly announced, they allow Bob and Alice to pick the sequence of bits associated with them as their private encryption key. Crucially, for complicated reasons that have to do with the nature of the protocol, this scheme does not require near-perfect detectors.

Moreover, as the two groups report in the latest issue of *Physical Review Letters*, it works even if the connecting optical fibres become long enough to be of practical use. Dr Rubenok and her

team have tested their version of the scheme on a spool of optical fibre more than 80km (50 miles) long, and also on 18km of working cable installed in Calgary. Dr Liu and Dr Chen have run it successfully over a link 50km long.

It all therefore looks quite promising. Unlike prepare-and-measure cryptography, no tinkering with the photon-generator could go undetected. But inevitably, there is a wrinkle. As Jonathan Barrett, another Oxford academic, points out, the interception need not take place in this bit of the system at all. Instead, the detector Alice bought from a manufacturer subverted by Eve could surreptitiously record the quantum-key data Alice receives, store them in a conventional memory, and then broadcast them to Eve later. That would enable her to decode Alice's earlier messages to Bob.

Dr Ekert reckons this threat is more theoretical than real. The non-quantum parts of the system, whose weakness Dr Barrett is pointing out, are easier to test for interference than the quantum parts that prepare-and-measure bugs hide in—and anyone concerned enough about security to bother with quantum cryptography in the first place is certainly going to scrutinise his equipment pretty thoroughly before he uses it. Soon, then, those who wish to communicate completely privily may be able to do so, whatever the world's Eves might try throwing at them.

"Based on the reading, describe the theory behind a quantum encryption and the solutions in work to fix some of the known issues with the encryption. Support your description with specific references and describe in detail where quantum encryption could be used in your life."